October 18, 2013 Release # 237

-- Begin Transmission --

The Risks of Using Portable Devices – Part 3

Being small and portable is another potential risk in both storage and smart devices as you might unintentionally leave them attached to the computer in an internet cafe or hotel room where you used them. Personal sensitive or proprietary organizational data might be compromised if the data or the devices are not encrypted.

What to Do to Minimize These Risks

Whether you are a home or an office user, there are things you can do to reduce the risks while using portable devices.

Recommended Practices for Portable Storage Media

- Install anti-virus software that will scan any device that connects to your PC via a peripheral port (such as USB).
- Never connect unknown or unauthorized usb device to a PC.
- Disable the Autorun and Autoplay features for all removable media devices. These features automatically open removable media when it's plugged into your USB port or inserted into a drive.
- Secure all sensitive data stored on jump drives, CDs, and DVDs using strong encryption, such as AES 128/256 bit1. Also be sure to have a backup copy located in a secure location.
- On your PC (and all PCs on a network), set up a firewall and install anti-virus and antispyware software. Enable automatic updates or otherwise ensure all software on your PC stays up to date with current patches.
- When you have finished transferring sensitive data from a USB drive, be sure to delete it using a secure delete utility.
- Consider using jump drives that have an onboard anti-virus capability, which automatically scans both the drive and any computer you plug it into. Although such a capability can take substantial disk space and time to run, it may be worth using, depending on your situation.

-- End of Transmission –

Information Security: It's a Shared Responsibility

REFERENCE(S): http://www.us-cert.gov/